UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Subject Accounts, as described in Attachments A-1 through A-5	)	Case No. MJ17-473

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachments A-1 through A-5, which are attached hereto and incorporated herein by this reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachments B-1 through B-5, which are attached hereto and incorporated by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
26 U.S.C. 7201, 7206	Tax Evasion, Filing a False Tax Return, Aiding or Assisting False Tax Returns
18 U.S.C. 371, 1341, 1343, 1028A, 1956, 1957	Conspiracy to Defraud the U.S., Mail Fraud, Wire Fraud, Aggravated Identity Theft, Money Laundering

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Eric Hergert

Applicant's signature

ERIC HERGERT, SPECIAL AGENT, IRS

Printed name and title

Sworn to before me pursuant to CrimRule 4.1.

Date: 11/14/17

Judge's signature

City and state: SEATTLE, WASHINGTON

Brian A. Tsuchida, U.S. MAGISTRATE JUDGE

Printed name and title

USAO 2016R00339

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Eric Hergert, a Special Agent with Internal Revenue Service, Criminal Investigation ("IRS-CI"), in Tacoma, Washington, having been duly sworn, state as follows:

I. INTRODUCTION

1. I make this Affidavit in support of an Application under Rule 41 for the Federal Rules of Criminal Procedure for search warrants for information associated with the following email and social media accounts (SUBJECT ACCOUNTS):

a. robbcrson@gmail.com

b. Robbcrson01@gmail.com

c. smtpreceiverinbox@gmail.com

d. Palmer.eloho.blogger@gmail.com

e. officialnomzky@gmail.com

f. nomzkysdmusiq@gmail.com

g. mailpami4ever@yahoo.com

h. Williamdotson38@yahoo.com

i. nomzkysdm@yahoo.com

j. onomen4us@yahoo.com

k. All Facebook accounts associated with the email address, mailpami4ever@yahoo.com, including the account with the Profile ID: 674058280

l. All Facebook accounts associated with the email address, onomen4us@yahoo.com, including the account with the Profile ID: 696285991

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

m. All Instagram accounts associated with the email address, mailpami4ever@yahoo.com, including the account with the Profile ID: 4268933941

n. All Instagram accounts associated with the email address, nomzkymusiq@gmail.com, including the account with the Profile ID: 209706106

o. All Twitter accounts associated with the email address, mailpami4ever@yahoo.com, including the account with the user name, "@palmerjoel88"

p. All Twitter accounts associated with the email address, officialnomzky@gmail.com, including the account with the account ID: 138361510 (collectively, "SUBJECT ACCOUNTS"). These accounts are further described in Attachments A-1 through A-5 (collectively, Attachments A) for the items described in Attachments B-1 through B-5 (collectively, Attachments B). These attachments are attached hereto and incorporated herein by this reference.

2. The information associated with the SUBJECT ACCOUNTS are stored at premises controlled by the following companies (collectively, SERVICE PROVIDERS):

a. Google, Inc., an email provider headquartered in Mountain View, California;

b. Yahoo!, Inc., an email provider headquartered in Sunnyvale, California;

c. Facebook, Inc., a social networking company headquartered in Menlo Park, California;

d. Instagram, LLC, a social-networking company owned by Facebook, Inc. and headquartered in San Francisco, California; or

e. Twitter, a social-networking company headquartered in San Francisco, California.

3. The information to be searched is described in the following paragraphs and in Attachments A. This affidavit is made in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the SERVICE PROVIDERS to disclose to the government copies of the information

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(including the content of communications) further described in Section I of Attachments B. Upon receipt of the information described in Section I of Attachments B, government-authorized persons will review that information to locate the items described in Section II of Attachments B.

4. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§2703(a), (b)(1)(a), and (c)(1)(a). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offenses being investigated." 18 U.S.C. § 2711(3)(a)(i).

5. As explained in the paragraphs below, there is probable cause to believe that the SUBJECT ACCOUNTS are either used almost exclusively in furtherance of criminal activity or are used exclusively by the perpetrators of the criminal scheme in question. More specifically, I have already searched the email accounts mailpami4ever@yahoo.com, robbcrson@gmail.com, williamdotson38@gmail.com, and smtpreceiverinbox@gmail.com, and have found extensive communications involving the scheme under investigation (e.g., "phishing" emails to extract sensitive tax records, payment information regarding tax refunds), and almost no personal communications. With regard to the remaining SUBJECT ACCOUNTS, information produced by the electronic communications providers for those accounts establishes probable cause to believe that the users of those accounts are the two individuals who use the robbcrson@gmail.com and mailpami4ever@yahoo.com accounts, both of which are used extensively in furtherance of the fraudulent scheme. On this basis, I respectfully submit that the Government should be permitted to search the accounts without waiving the "plain view" doctrine or using a "filter" team.

II. SPECIAL AGENT BACKGROUND

6. I am a Special Agent with IRS-CI, and have been so employed since September 2009. I am presently assigned to IRS-CI's Seattle Field Office. My duties and responsibilities include the investigation of possible criminal violations of the Internal Revenue laws (Title 26, United States Code), the Bank Secrecy Act (Title 31,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

United States Code), the Money Laundering Control Act of 1986 (Title 18, United States Code, Sections 1956 and 1957), and other related offenses.

7. I earned a Bachelor of Arts degree in accounting from the University of Washington, Tacoma, in 2002. I attended the Criminal Investigator Training Program and the IRS Special Agent Basic Training at the Federal Law Enforcement Training Center where I received detailed training in conducting financial investigations. The training included search and seizure, the Internal Revenue laws, and IRS procedures and policies in criminal investigations. Before being hired by IRS-CI, I was employed as a Revenue Agent for the IRS for approximately five years, performing civil examinations of small businesses and self-employed individuals. As a Revenue Agent, I received approximately 16 weeks of specialized training in personal, partnership, and corporate income tax, as specified in the Internal Revenue Code.

8. I have conducted and assisted in several investigations involving financial crimes. I have led and participated in the execution of search warrants and have interviewed witnesses and defendants who were involved in, or had knowledge of, violations of the Internal Revenue Code, the Bank Secrecy Act, and the Money Laundering Control Act. In the course of my employment with IRS-CI, I have conducted and have been involved in investigations of alleged criminal violations, which have included tax evasion (26 U.S.C. § 7201), filing a false tax return (26 U.S.C. § 7206(1)), aiding or assisting in the preparation of false tax returns (26 U.S.C. § 7206(2)), conspiring to defraud the United States (18 U.S.C. § 371), wire and mail fraud (18 U.S.C. §§ 1343, 1341), aggravated identity theft (18 U.S.C. § 1028A), and money laundering (18 U.S.C. §§ 1956, 1957), among others.

9. I have led and participated in the execution of federal search warrants and the consensual searches of records relating to the concealment of assets and proceeds derived from fraud. These records included, but were not limited to, emails, instant messages, personal telephone books, photographs, bank records, escrow records, credit

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

card records, tax returns, business books and records, and computer hardware and software.

10. The information provided in this Affidavit is supported by my training, experience, education, and participation in this and other financial and identity theft investigations.

11. The facts set forth in this Affidavit are based on my personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, review of documents and records related to this investigation, communication with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. The information provided in this Affidavit is supported by my training, experience, education, and participation in this and other financial investigations.

12. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that violations of 18 U.S.C. § 371 (conspiracy), § 641 (theft of public money), § 1028A (aggravated identity theft), and § 1343 (wire fraud), collectively, the "Subject Offenses" have been committed by individuals known as Palmer Joel Eloho, Onomen Uduebor, and other unknown persons, and that evidence, instrumentalities, and fruits of such crimes will be found in the SUBJECT ACCOUNTS.

III. DEFINITION OF TERMS

13. The term "phishing" is defined by Merriam-Webster Dictionary as "a scam by which an email user is duped into revealing personal or confidential information which the scammer can use illicitly."

14. An "email header" is text at the beginning of an email message. It is generated by the client email program that first sends it and is updated by all the email

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

servers (i.e., computer programs or devices that provide functionality for other programs or devices) en route to the destination. Each email server adds more text, including from/to addresses, subject, content type, time stamp, and identification data. The path of the message from source to destination can be traced by reviewing the email header text. Many end-user email programs hide this information from the user unless the user specifically requests to view it.

15. An Internet cookie file, or "cookie," is a file that a website stores on a user's computer. The website can read the "cookie" and collect information about the computer on which the cookie has been saved. For example, a cookie might be used to track a user's account on the website, a user's preferences, or items in a user's electronic shopping cart.

16. The Internet Protocol ("IP") is the method or protocol by which data is sent from one computer to another on the Internet. Each computer on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

17. This Affidavit discusses tax returns in various stages of processing. When a return is initially received by the IRS, it is reviewed to ensure certain standards are met, such as if the Social Security Number ("SSN") is correct, if the date of birth is correct, and whether or not a tax return has previously been submitted for that individual. If the tax return passes this initial review, it is considered "accepted." If it fails, it is "rejected." Once a tax return has been accepted by the IRS, it undergoes additional review. During this review, a claimed refund payment may be withheld by the IRS if the tax return appears to be fraudulent or if there are identity theft concerns. If a refund payment is made pursuant to a tax return, that payment could still be stopped and returned to the IRS by a refund transfer service or bank receiving the refund if that institution believes the refund payment constitutes the proceeds of fraud.

18. Various "refund transfer services" will accept tax refunds for a client, pay off various return preparation fees, then forward the remaining refund to the bank account designated by the client. In effect, the refund transfer service works very similarly to an

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

escrow account. Since the issued refunds are not available to be used until forwarded by the refund transfer service to the designated bank account, they have been generally disregarded during the tracing of fraudulent refunds for the purpose of this Affidavit.

IV. SUMMARY OF THE INVESTIGATION

19. Beginning approximately February 2016, IRS-CI began receiving reports from several companies across the United States regarding phishing schemes. In these schemes, unknown individuals impersonated high-level management figures in emails sent to employees working in human resources or payroll processing. These emails requested the identity and payroll information of all company employees, often specifically requesting the IRS Form W-2, Wage and Tax Statement, information. In many instances, the human resources or payroll processing employee believed the phishing emails actually came from senior management and replied to the email with the requested information, thereby sharing the identity and payroll information for company employees with the perpetrators of the phishing scheme. The perpetrators of the fraud then used the personal information to file fraudulent tax returns in which they posed as the identity theft victims and requested tax refunds.

20. Onomen Uduebor and Palmer Joel Eloho have been identified as subjects in this case. Information detailed below show that they are involved in conducting phishing attacks and filing fraudulent tax returns with the IRS.

21. Although the names of Onomen Uduebor and Palmer Joel Eloho have been identified, very little other information about them has been identified at this time. Information obtained through this search warrant is expected to provide additional evidence regarding the identity of these individuals, as well as provide evidence of their involvement in the scheme.

22. The identity of any additional subjects behind the scheme is not known at this time.

23. On December 19, 2016, the Honorable Brian A. Tsuchida, United States Magistrate Judge, issued search warrants for several email accounts, including some of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the email accounts that are the subject of this application. My Affidavit in support of those search warrants is attached hereto as Exhibit A and incorporated herein by this reference.[1]

V. STATEMENT OF PROBABLE CAUSE

A. Review of Materials Found In robbcrson@gmail.com

24. On or about December 19, 2016, I served Google, Inc. with a search warrant issued by the Honorable Brian A. Tsuchida under cause number MJ16-531 for information contained within the email account, robbcrson@gmail.com. The materials found in the email account, which was created on October 24, 2013, confirms that it was used in connection with a scheme to commit tax fraud, by inducing companies to disclose their employees' W-2 information.[2]

25. The robbcrson@gmail.com email account was opened on October 24, 2013. The subscriber provided Google, Inc. with the alternate email account, nomzkysdm@yahoo.com, and the phone number +234-8090-602436, a phone number that appears to be from Nigeria. The same telephone number was provided to Yahoo by the user of the williamdotson38@yahoo.com account (which is described in additional detail in Exhibit A, and which was one of the accounts that the warrants issued on December 19, 2016 authorized law enforcement agents to search).[3] According to information provided by Google, Inc., the same device was used to access the robbcrson@gmail.com email account and the officialnomzky@gmail.com email account.

---

[1] Paragraph 25 of Exhibit A made reference to 24 suspicious returns and 75 fraudulent and suspicious returns. Those references should state that there were 23 suspicious returns and 74 fraudulent and suspicious returns. In addition, paragraph 46 of Exhibit A makes reference to 33 W-2 forms sent by "K.W." The reference to "K.W." should, in fact, read "J.P." In addition, paragraph 28 of Exhibit A referred to 25 suspicious returns relating to Idexcel, Inc. and claimed refunds of $305,575. Those references should state that there were 24 suspicious returns and a claimed amount of $305,066. Finally, paragraph 33 of Exhibit A refers to 58 returns relating to Alpine Learning Group, Inc. That reference should be to 59 returns.

[2] My review of the email messages provided by Google, Inc. for the robbcrson@gmail.com account found substantially no personal communication. The messages were related to various fraudulent schemes, included the scheme discussed in this affidavit, or various commercial advertisement messages.

[3] Indeed, the user of williamdotson38@yahoo.com provided Yahoo with robbcrson@gmail.com as a back-up email address for the account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

26. I found copies of over 2,100 emails, dated February through May, 2016, that appeared to be spam phishing attacks. These attacks included both attempts to steal Forms W-2 from six different companies, as well as attempts to trick companies into sending money into bank accounts controlled by members of the scheme. For example:

a. On or about March 7, 2016, the robbcrson@gmail.com email account received approximately 148 copies of phishing attack email messages with the subject lines "Request for Employees' 2015 W2" or "Peruse: Request for Employees' W2." These messages included copies of the phishing emails referred to above and in Exhibit A, which were sent to Workforce Software, LLC, MTE Corporation, and ASF Logistics, Inc. In my training and experience, it is notable that the robbcrson@gmail.com account held copies of emails that were sent to different companies, from different email addresses, and from different purported senders. It suggests that the user of the robbcrson@gmail.com account used different email accounts to send those phishing emails and kept a record of those emails in his main account.

b. On or about February 26, 2016, the robbcrson@gmail.com email account received approximately 52 copies of phishing attack email messages with the subject line, "Peruse: Request for Employees' W2." As with the emails described with sub-paragraph (b) above, these emails had been sent to different companies (namely, Pritchard Industries SW, Inc., Mansueto Ventures, LLC, and Control Air Conditioning Corp.), from different email addresses, and from different purported senders. The emails included similar language requesting that employees at the victim companies disclose information about the companies' employees' W-2s. Thus, these emails also suggest to me that the user of robbcrson@gmail.com used different email accounts to send phishing emails and then kept a record of those emails in his main account.

27. I also found over 300 email messages, dated February through May, 2016, that appeared to contain personally-identifying information and other tax return filing information, and approximately 130 email messages that appeared to contain bank or prepaid debit card account information.[4] Based on my training and experience, these bank and prepaid debit card accounts were likely opened using stolen identity

[4] During my review of the messages in the robbcrson@gmail.com account, I noted that Google, Inc. did not provide any email messages that included attachments. When I asked a Google, Inc. representative about this, they stated the emails with attachments were not provided because they could not verify the attachments were stored on computer servers in the United States

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information, or by unwitting individuals tricked into providing their banking information to the identity thieves through various types of online scams.

28. I have taken steps to identify the user of the robbcrson@gmail.com and to identify other web-based accounts used by that person.

a. ***First,*** I have developed probable cause to believe that the same person who uses the robbcrsn Gmail address also uses a Twitter account with the account name (or "handle") of "@officialnomzky." I first discovered the Twitter account "@officialnomzky" by searching online for Twitter accounts with the user name "nomzky," in light of the repeated references to that screenname in other search warrant returns. According to subscriber information provided by Twitter, the account was opened April 29, 2010 with the account ID is 138361510, and the subscriber associated the Twitter account with the email account officialnomzky@gmail.com and the phone number +234-8090-602436. The subscriber details also list the user as being in "West Central Africa". Additionally, when I viewed the @officialnomzky Twitter "page", I found the page was for a performing artist that goes by the stage name, "Nomzky." Listed on the Twitter page as of September 13, 2017, in the user information section, was the email address, nomzkysdmusiq@gmail.com.

b. ***Second***, I have developed probable cause to believe that the same person who uses the robbcrson@gmail.com email address also uses the email addresses nomzskydmusiq@gmail.com and nomzkysdm@yahoo.com As set out above, the Twitter page for "@officialnomzsky" lists nomzskydmusiq@gmail.com as the email address associated with the Twitter account. In addition, subscriber information produced by Google, Inc. for the email account nomzkysdmusiq@gmail.com listed nomzkysdm@yahoo.com as the recovery email account and listed the phone number +234-9099-044458 as the subscriber's phone number. As set out above, the email address nomzkysdm@yahoo.com is also the same recovery email address that the user of robbcrson@gmail.com provided to Google, Inc.

c. ***Third***, I have developed probable cause to believe that the same person who uses the robbcrson@gmail.com account also uses an account on Instagram, a social-media website that enables users to share photographs and videos, with profile ID number 209706106 bearing the user name (or "vanity name") of "officialnomzsky." Specifically, information provided by Instagram, LLC shows that the email address nomzkysdmusiq@gmail.com was used as the registration email address for an "Instagram page" user with the profile id number 209706106.

d. ***Fifth***, I have developed probable cause to believe that the user of robbcrson@gmail.com operates a Facebook account with profile ID number 696285991 and user name "nomzky." Specifically, the robbcrson@gmail.com account included email messages sent to and received from a person named Onomen Uduebor, using the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

email account onomen4us@yahoo.com. Publicly available information on the internet shows that the name "Onomen Uduebor" is the name of a Nigerian musician who goes by the alias "nomzky." Records produced by Facebook show that the email address onomen4us@yahoo.com was used as the registration email address for a "Facebook page" user with the profile id number 696285991. As of July 14, 2017, the account used the vanity name, "nomzky". The account was registered with the subscriber name "Onomen Nomzky". The subscriber also provided Facebook, Inc. with the phone number +234-9099-044458 as a phone number for the user.

29. Based on the information described above, there is probable cause to believe Onomen Uduebor uses all of these accounts and is located in Nigeria. There is also probable cause to believe that evidence of the Subject Offenses will be found on these accounts, insofar as the accounts already have been used extensively in furtherance of the criminal scheme, will corroborate the identity of the person associated with the criminal scheme, will identify potential co-conspirators in the criminal scheme by showing who Uduebor corresponded with, and will provide agents with information about the location of the participants in the criminal scheme at or around the times that they engaged in the criminal conduct:

a. Williamdotson38@yahoo.com email account

b. officialnomzky@gmail.com email account

c. Nomzkysdmusiq@gmail.com email account

d. nomzkysdm@yahoo.com email account

e. Onomen4us@yahoo.com email account

f. nomzky Facebook.com account (profile ID 696285991)

g. officialnomzky Instagram.com account (profile ID 209706106)

h. @officialnomzky Twitter account (account ID 138361510)

B. Review of Materials Found In mailpami4ever@yahoo.com

30. On or about December 19, 2016, I served Yahoo!, Inc. with a search warrant issued by the Honorable Brian A. Tsuchida under cause number MJ16-533 for information contained in the email account mailpami4ever@yahoo.com. The materials found in the email account, which was created on February 19, 2007, confirms that it was

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

used in connection with a scheme to commit tax fraud, by inducing companies to disclose their employees' W-2 information.[5] In particular, I found approximately 158 messages in the mailpami4ever@yahoo.com account (including incoming and outgoing messages) between February 26, 2016 and May 13, 2016, many of which were associated with the alleged fraud under investigation.[6]

31. Records produced by Yahoo!, Inc. ("Yahoo") show that the mailpami4ever@yahoo.com email account was opened on February 19, 2007. The subscriber used the name "Mr Eloho palmer," and indicated his country of residence was Nigeria. Email messages in the account referred to the names "Palmer Eloho", "Eloho Palmer", "Joel Palmer" in a self-referential manner – e.g., in an email message sent by mailpami4ever@yahoo.com dated February 10, 2013 the sender referred to himself as "Eloho Palmer," stated that he was in Nigeria, and included photographs that he claimed to be of himself. As part of their response to the above mentioned search warrant, Yahoo included subscriber information on several email accounts associated with mailpami4ever@yahoo.com, which establishes a connection between the various accounts (as discussed in additional detail below).

32. Approximately 46 messages in the mailpami4ever@yahoo.com account included an attachment, which contained Forms W-2 associated with employees of the companies that were victimized by the phishing scheme discussed above and in Exhibit A (as well as another three companies that I had not previously identified as victims of the scheme). For example:

a. On February 26, 2016, mailpami4ever@yahoo.com (along with robbcrson@gmail.com and two other email addresses) received an email from another email account used in the scheme: chair.man@execs.com. The chair.man@execs.com email account forwarded to mailpami4ever@yahoo.com an email from the payroll

---

[5] My review of the email messages provided by Google, Inc. for the mailpami4ever@yahoo.com account found substantially no personal communication. The messages were related to various fraudulent schemes, included the scheme discussed in this affidavit, or various commercial advertisement messages.

[6] Outside of this date range, there were several other email messages in the mailpami4ever@yahoo.com account indicative of fraud, namely email messages regarding (i) lottery scams, (ii) impersonation scams designed to induce businesses to transfer unwittingly money to bank accounts; and (iii) scams designed to induce victims to disclose unwittingly their privately identifiable information and bank account information.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

manager at Mansueto Ventures, LLC, a company in New York. The Mansueto Ventures payroll manager, in apparent response to a phishing email, had sent chair.man@execs.com W-2 information for 372 employees. In my training and experience, the fact that the payroll manager's email was forwarded by chair.man@execs.com to mailpami4ever@yahoo.com and other email addresses is consistent with the use of chair.man@execs.com as a "front" to conduct the fraud scheme.[7]

b. On February 26, 2016, mailpami4ever@yahoo.com received an email from robbcrson@gmail.com with an attachment that included approximately 2,230 W-2 forms for the 2015 tax year for employees of Pritchard Industries SW, Inc., a company in New York, New York.[8]

c. Beginning on approximately March 1, 2016, the mailpami4ever@yahoo.com email account received various email messages that included Forms W-2, or Form W-2 information for employees of Control Air Conditioning Corp. and Control Air North, Inc., both located in Anaheim, California.[9]

33. I also found 57 other email messages that contained information regarding filing fraudulent tax returns. These messages included information such as the identity theft victims' personally identifiable information (PII) and employment information, IRS PIN numbers to be used in the filing of the tax returns, login information for tax preparation websites, the amounts of the tax refunds, and bank accounts to be used to receive the fraudulent tax refunds.

---

[7] I reviewed IRS records on September 11, 2017 to determine whether any of those W-2s may have been used to file fraudulent federal income tax returns. From February 26, 2016 to the end of the year, the IRS accepted approximately 271 electronically filed tax returns that included Forms W-2 reporting income from Mansueto Ventures, LLC. As of my review, the IRS determined that 37 of the tax returns were fraudulent, and an additional 13 were suspicious and pending further review due to potential identity theft concerns. These 50 fraudulent and suspicious tax returns claimed refunds totaling $121,323.

[8] I reviewed IRS records on September 11, 2017 to determine whether those W-2s may have been used to file fraudulent federal income tax returns. I found that, between February 26, 2016 and the end of 2016, the IRS accepted approximately 886 electronically filed tax returns that included Forms W-2 reporting income from Pritchard Industries SW, Inc. As of my review, the IRS determined that 32 of the tax returns were fraudulent, and an additional six were suspicious and pending further review due to potential identity theft concerns. These 38 fraudulent and suspicious tax returns claimed refunds totaling $106,313.

[9] On September 11, 2017, I conducted a review of IRS records to determine the status of tax returns filed in 2016 reporting wage income from Control Air Conditioning Corp and Control Air North, Inc. From February 26, 2016 to the end of the year, the IRS accepted approximately 508 electronically filed tax returns that included Forms W-2 reporting income from Control Air Conditioning Corp and Control Air North, Inc. As of my review, the IRS determined that 37 of the tax returns were fraudulent, and an additional 21 were suspicious and pending further review due to potential identity theft concerns. These 58 fraudulent and suspicious tax returns claimed refunds totaling $246,958.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

34. I also found 15 email messages, which contained information regarding bank accounts or prepaid debit card accounts opened many different names. Based on my training and experience, these accounts were likely opened using stolen identity information, or by unwitting individuals tricked into providing their banking information to the identity thieves through various types of online scams.

35. There is probable cause to believe that the user of mailpami4ever@yahoo.com also uses the email account palmer.eloho.blogger@gmail.com. Specifically, the user of mailpami4ever@yahoo.com account provided Yahoo with palmer.eloho.blogger@gmail.com, which he designated as an "alternate communications channel." I found an email message from Google, Inc. in the mailpami4ever@yahoo.com account, which addressed the creation of the palmer.eloho.blogger@gmail.com account. Records produced by Google establish that palmer.eloho.blogger@gmail.com was created on March 1, 2013, with the subscriber name "palmer eloho," and the recovery email address mailpami4ever@yahoo.com. Google, Inc. also produced records showing that the digital devices that accessed palmer.eloho.blogger@gmail.com were the same digital devices that Google previously identified as having accessed smtpreceiverinbox@gmail.com, which is one of the email accounts to which stolen Form W-2s were forwarded by headquarter@accountant.com.

36. There is also probable cause to believe that the user of mailpami4ever@yahoo.com also uses a Facebook account with profile ID number 674058280 and the user name "palmer.eloho." Specifically, information provided by Facebook, Inc. showed the email address mailpami4ever@yahoo.com was used as the registration email address for a "Facebook page" user with the profile id number 674058280. As of July 14, 2017, the account used the vanity name, "palmer.eloho". The account was registered with the subscriber name "Palmer Joel Eloho". On September 12, 2017, I reviewed the publicly viewable photographs posted by the account user and was able to identify both photographs as the same ones included in the February 10, 2013

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

email message sent from the mailpamiforever@yahoo.com account. Several other photographs posted by the user of the account appear to be of the same person.

37. There is also probable cause to believe that the user of mailpami4ever@yahoo.com also uses an Instagram account with profile ID number 4268933941 and the user name "therealdoc80." Specifically, information provided by Instagram, LLC showed the email address mailpami4ever@yahoo.com was used as the registration email address for an "Instagram page" user with the profile id number 4268933941. As of July 14, 2017, the account used the vanity name "therealdoc80". The account was registered with the subscriber name "Palmer Joel Eloho". Some of the photographs on this account also appear to be of the same person as in the photographs in the February 10, 2013 email message from the mailpami4ever@yahoo.com account and the palmer.eloho account on Facebook.com. Additionally, on July 21, 2017, this user commented on a post, stating that he was in Lagos, Nigeria.

38. Finally, there is probable cause to believe that the user of mailpami4ever@yahoo.com also uses a Twitter account with the handle "@palmerjoel88." Specifically, during my review of the mailpami4ever@yahoo.com account, I found several email messages from Twitter, Inc. to the purported user of the Twitter account "@palmerjoel88." In my training and experience, Twitter emails its users at the email address that they have registered in connection with their Twitter accounts. Additionally, this twitter account was claimed in at least two posts on the "Facebook page" for the palmer.eloho account.

39. Based on the information described above, there is probable cause to believe that the user of the mailpami4ever@yahoo.com account is also the sole user of the email and social media accounts set out below. There is probable cause to believe that Palmer Joel Eloho uses all of these accounts and is located in Nigeria. Finally, there is probable cause to believe that evidence of the Subject Offenses will be found on these accounts, insofar as the accounts already have been used extensively in furtherance of the criminal scheme, will corroborate the identity of the person associated with the criminal

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

scheme, will identify potential co-conspirators in the criminal scheme by showing who Eloho corresponded with, and will provide agents with information about the location of the participants in the criminal scheme at or around the times that they engaged in the criminal conduct.

a. palmer.eloho.blogger@gmail.com email account

b. palmer.eloho Facebook.com account (profile ID 674058280)

c. therealdoc80 Instagram.com account (profile ID 4268933941)

d. @palmerjoel88 Twitter account

VI. TRAINING AND EXPERIENCE IN STOLEN IDENTITY REFUND FRAUD INVESTIGATIONS

40. Based on my training and experience, conversations with other law enforcement officers conducting SIRF (Stolen Identity Refund Fraud) investigations, my participation in this and other SIRF investigations, and my examination of reports and evidence in this and other SIRF investigations, I know that SIRF offenses are frequently continuing criminal enterprises which span over months and, often, years. Individuals involved in SIRF regularly obtain PII of other persons, including tax and other financial information, and use the PII to file fraudulent tax refund requests to the IRS.

41. Perpetrators of SIRF schemes typically store the PII and tax refund request information on not only their digital devices, but also in their email accounts and other remote storage locations. In addition to those email accounts, the perpetrators of SIRF scheme also use other messaging applications, including messaging capabilities available through social-media applications like Facebook, Twitter, and Instagram. Those messaging applications enable perpetrators of the scheme to share information with other co-conspirators, and identify targets.

42. Since SIRF often is an ongoing criminal enterprise, individuals involved typically will keep additional records associated with their illegal activities for an extended period of time, especially since such records are vital to the orderly operation of the enterprise. Such records are typically kept in the residences, places of business, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

email accounts of the persons involved in SIRF. In my experience, the records kept by these individuals include:

a. Documents and other information related to the preparation of fraudulent tax returns and/or tax laws, such as IRS publications, forms, or documents, and any correspondence relating to tax returns.

b. Information obtained from the IRS website, including tools that the IRS offers to taxpayers in order to facilitate the filing of electronic returns.

c. Records, including electronic records, documents, and information that relate to the acquisition or use of tax preparation software.

d. Prepaid debit cards and associated records, credit cards, magnetic card stock, gift cards, or other cards with magnetic strips readable by credit card processing equipment, equipment to read and/or write magnetic strip information onto magnetic cards, bank statements, Western Union, MoneyGram, or similar receipts, money order receipts, cash deposit and withdrawal receipts, bank or wire transfer records, casino cash in/out records, utility bills, lease documents, safety deposit box records and keys, and other similar documents or items.

e. Records, such as instructions and guides, relating to the process of stealing identity information and using it in the context of a SIRF or other scheme relating to identity theft.

f. Address books, contact lists, personal calendars, diaries, photographs, videos, documents, programs, applications, or other similar records, such as those which reflect the identities of any co-conspirators, accomplices, or aiders and abettors in the commission of the Subject Offenses.

g. Billing statements, purchase records, calling history, and related information for cellular telephones, residential telephones, Internet services, and other communication devices and services.

h. Records of any communication involving the exchange or acquisition of information and identifiers of businesses/employers or belonging to third

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

party persons and victims of identity theft or other communication involved in committing the Subject Offenses, including communication regarding hackers.

43. Based on my training and experience, I know that SIRF is often conducted by groups of individuals. These individuals may be in different locations across the country, or even in different countries across the world. In order to conduct the scheme, the co-conspirators have to communicate. This communication is often done through text messages, emails, and instant messenger accounts. In this case specifically, I have conducted search warrants of several email accounts. These accounts appear to be the primary method of transferring stolen Forms W-2, instructions, and other information to be used for SIRF. The email messages searched with regards to this investigation provide strong indications there are multiple people involved. For example, there are emails and instant messages between email accounts that ask and answer questions or provide directions on how to advance the scheme.

44. From my background and training I generally know that email, instant messaging, text messaging, and other forms of electronic communication are often used by criminal organizations to facilitate SIRF crimes. I have reviewed information obtained from search warrants of email and instant message accounts and know that these forms of communication are often used by identity thieves to obtain and transfer:

a. Identity theft victims' PII, such as name, SSN, address, and date of birth;

b. Credit reports, income information, and prior year tax return information of identity theft victims;

c. Passwords, PIN numbers, and other information required to file fraudulent tax returns in the names of identity theft victims;

d. Bank and prepaid debit card account numbers and passwords;

e. Instructions on how to obtain PII, file fraudulent returns, and access the fraudulent refunds; and

f. Instructions on how to disperse the fraudulent refunds received.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

45. There are many reasons why criminal offenders maintain electronic communication evidence for long periods of time. Items such as identity theft victim PII have value, as they may be sold, used for other purposes, or reused for the same purpose in future years. Additionally, electronic communication is often stored on third party servers, and may not actually be deleted immediately, even if put into a "deleted items folder" or "trash." The criminal offender may no longer realize that they still possess the evidence or they may believe that law enforcement could not obtain a search warrant to seize the evidence.

46. In many instances, identity thieves also communicate with individuals not involved in the conspiracy for purposes of using them unwittingly in their scheme. For example, identity thieves will befriend individuals met through online dating sites and convince them to receive money from a source unknown to that person and forward it on to the identity thief. Although the identity thief usually uses a false identity in these email communications, the items being discussed could provide information or evidence that can be used to further identify the identity thief or trace the fraudulent refunds.

47. Based on my training and experience, I also know that identity thieves often use email to communicate about other matters that may provide evidence as to the identity and location of the individual(s) using the email accounts. I know that communications between identity thieves may also include identifying information about the users of the email or instant message accounts. For example, messages may include names, nicknames, locations, travel plans, or birthdays that can be used to identify the criminal offenders.

48. Based on my training and experience, I know that individuals conducting phishing schemes, identity theft, and SIRF crimes often have several email addresses. The multiple email accounts are used because accounts often get closed by the email providers when they receive information regarding the email account being used in phishing schemes.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

49. Email and social media accounts used by the individuals conducting the phishing, identity theft, and tax fraud schemes for non-criminal communication may still contain evidence of the identity of the individual(s) using the accounts. This evidence is crucial in identifying the subjects using the accounts.

VII. BACKGROUND REGARDING EMAIL PROVIDERS' SERVICES

50. In my training and experience, I have learned that Google, Inc. and Yahoo!, Inc. (collectively, EMAIL PROVIDERS) provide the public with a variety of on-line services, including electronic mail ("email") access, to the public. The EMAIL PROVIDERS allow subscribers to obtain email accounts under various domain names, including gmail.com for Google, Inc. and yahoo.com for Yahoo!, Inc., like the email accounts listed in Attachments A. Subscribers obtain an account by registering with the EMAIL PROVIDERS. During the registration process, the EMAIL PROVIDERS ask subscribers to provide basic personal information, which may include name, address, phone numbers, payment information, and other personal information. Therefore, the computers of the EMAIL PROVIDERS are likely to contain stored electronic communications (including retrieved and unretrieved email for the EMAIL PROVIDERS' subscribers) and information concerning subscribers and their use of the EMAIL PROVIDERS' services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

51. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

52. In general, an email that is sent to an EMAIL PROVIDERS subscriber is stored in the subscriber's "mail box" on the EMAIL PROVIDERS' servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the EMAIL PROVIDERS' servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the EMAIL PROVIDERS' servers for a certain period of time.

53. When subscribers send emails, they are initiated at the users' computers, transferred via the Internet to the EMAIL PROVIDERS' servers, and then transmitted to their end destinations. The EMAIL PROVIDERS often maintain a copy of the email sent. Unless the email senders specifically delete the emails from the EMAIL PROVIDERS' servers, the emails can remain on the systems indefinitely. Even if the senders delete the emails, they may continue to be available on the EMAIL PROVIDERS' servers for a certain period of time.

54. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by the EMAIL PROVIDERS but may not include all of these categories of data.

55. Subscribers to the EMAIL PROVIDERS services can also store files, including emails, address books, contact or buddy lists, calendar data, photographs, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

other files, on servers maintained and/or owned by the EMAIL PROVIDERS. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, attachments to emails, including photographs and files, and photographs and files stored in relation to the account.

56. A Yahoo, Inc. subscriber can also store files, including emails, address books, contact or buddy lists, calendar data, photographs, and other files, on servers maintained and/or owned by Yahoo, Inc. I know based on my training and experience, and my review of Yahoo's services, that Yahoo! provides users with access to an address book in which they may store contact information including names, addresses, email address, and telephone numbers. Yahoo! also provides users access to a "Calendar" file that may include notes of events and schedules. Yahoo also provides users with access to a service called "Flicker" that can be used to create photo albums, store photographs, and share photographs with others. Yahoo! also provides users with access to Yahoo! Groups which allows users to share photographs, calendars and messages with others who typically share a common interest. In my training and experience, evidence of who was using an email account may be found in address books, calendars, photographs and other documents stored in relation to the account.

57. A subscriber to a Google Gmail account can also store files, including address books, contact lists, calendar data, photographs and other files, on servers maintained and/or owned by Google. For example, Google offers users a calendar service that users may utilize to organize their schedule and share events with others. Google also offers users' a service called Google Drive that may be used to store data and documents. The Google Drive service may be used to store documents including spreadsheets, written documents (such as Word or Word Perfect) and other documents that could be used to manage a website. Google Drive allows users to share their documents with others or the public depending on the settings selected by the account holder. Google also provides its users with access to the photo storage service "Picasa."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Picasa can be used to create photo albums, store photographs, and share photographs with others. Another Google service called "You Tube" allows users to view, store and share videos. Google also provides a service called "Google Analytics. Google Analytics is a Google service that monitors website traffic and provides subscribers with data relating to how much traffic is visiting the subscriber's website, which sections of the subscriber's website users are visiting, how long users are staying on particular sections of the site, and the geographical source of users visiting the website, among other things.

58. Additionally, based on my training and experience, as well as Google, Inc.'s Privacy Policy, I know that Google, Inc. also collects information about users, including information about the devices on which they access their accounts, the devices' hardware models, operating system versions, unique device identifiers, and mobile network information including phone number, location information, and search queries. This information is evidence that can be used to identify and find the individuals conducting the fraud.

59. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

60. This application seeks a warrant to search all responsive records and information under the control of the EMAIL PROVIDERS, providers subject to the jurisdiction of this court, regardless of where the EMAIL PROVIDERS have chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

record, or other information is within the EMAIL PROVIDERS' possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

61. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

62. Based on my training and experience, I know that some email providers, including the EMAIL PROVIDERS, often use internet cookie files to track user information. These "cookies" may allow the email providers to collect information about the account users' computers, including information about other accounts accessed by a computer containing the email provider's "cookie." Specifically, the EMAIL PROVIDERS may collect information about other email accounts with their service that were accessed by the computers that also accessed the email accounts described in Attachments A.

63. Information regarding other email accounts accessed from the same computer(s) that accessed the email accounts described in Attachments A may provide important evidence about the person using both accounts, including his/her identity and location, as well as the full extent of the fraud.

VIII. BACKGROUND REGARDING FACEBOOK SERVICES

64. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

65. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

66. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

67. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

68. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

69. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

70. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

71. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

72. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

73. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

74. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

75. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

76. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

77. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

78. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

79. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

80. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

81. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

82. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

IX. BACKGROUND REGARDIG INSTAGRAM SERVICES

83. From my review of publicly available information provided by Instagram about its service, including Instagram's "Privacy Policy," I am aware of the following about Instagram and about the information collected and retained by Instagram.

84. Instagram owns and operates a free-access social-networking website of the same name that can be accessed at http://www.instagram.com. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application ("app") created by the company that allows users to access the service through a mobile device.

85. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as certain other social-media services, including Flickr, Facebook, and Twitter. When posting or sharing a photo on Instagram, a user can add to the photo: a caption; various "tags" that can be used to search for the photo (e.g., a user made add the tag #vw so that people interested in Volkswagen vehicles can search for and find the photo); location information; and other information. A user can also apply a variety of "filters" or other visual effects that

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also "like" photos.

86. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. This information is collected and maintained by Instagram.

87. Instagram asks users to provide basic identity and contact information upon registration and also allows users to provide additional identity information for their user profile. This information may include the user's full name, e-mail addresses, and phone numbers, as well as potentially other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. Instagram collects and maintains this information.

88. Instagram allows users to have "friends," which are other individuals with whom the user can share information without making the information public. Friends on Instagram may come from either contact lists maintained by the user, other third-party social media websites and information, or searches conducted by the user on Instagram profiles. Instagram collects and maintains this information.

89. Instagram also allows users to "follow" another user, which means that they receive updates about posts made by the other user. Users may also "unfollow" users, that is, stop following them or block the, which prevents the blocked user from following that user.

90. Instagram allow users to post and share various types of user content, including photos, videos, captions, comments, and other materials. Instagram collects and maintains user content that users post to Instagram or share through Instagram.

91. Instagram users may send photos and videos to select individuals or groups via Instagram Direct. Information sent via Instagram Direct does not appear in a user's feed, search history, or profile.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

92. Users on Instagram may also search Instagram for other users or particular types of photos or other content.

93. For each user, Instagram also collects and retains information, called "log file" information, every time a user requests access to Instagram, whether through a web page or through an app. Among the log file information that Instagram's servers automatically record is the particular web requests, any Internet Protocol ("IP) address associated with the request, type of browser used, any referring/exit web pages and associated URLs, pages viewed, dates and times of access, and other information.

94. Instagram also collects and maintains "cookies," which are small text files containing a string of numbers that are placed on a user's computer or mobile device and that allows Instagram to collect information about how a user uses Instagram. For example, Instagram uses cookies to help users navigate between pages efficiently, to remember preferences, and to ensure advertisements are relevant to a user's interests.

95. Instagram also collects information on the particular devices used to access Instagram. In particular, Instagram may record "device identifiers," which includes data files and other information that may identify the particular electronic device that was used to access Instagram.

96. Instagram also collects other data associated with user content. For example, Instagram collects any "hashtags" associated with user content (i.e., keywords used), "geotags" that mark the location of a photo and which may include latitude and longitude information, comments on photos, and other information.

97. Instagram also may communicate with the user, by email or otherwise. Instagram collects and maintains copies of communications between Instagram and the user.

98. As explained herein, information stored in connection with an Instagram account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

my training and experience, an Instagram user's account activity, IP log, stored electronic communications, and other data retained by Instagram, can indicate who has used or controlled the Instagram account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Instagram account activity can show how and when the account was accessed or used. For example, as described herein, Instagram logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Instagram access, use, and events relating to the crime under investigation. Additionally, Instagram builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Instagram "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Instagram account owner. Last, Instagram account activity may provide relevant insight into the Instagram account owner's state of mind as it relates to the offense under investigation. For example, information on the Instagram account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

99. Based on the information above, the computers of Instagram are likely to contain all the material described above with respect to the SUBJECT ACCOUNTS, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, which would include

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

X. BACKGROUND REGARDING TWITTER SERVICES

100. Twitter owns and operates a free-access social-networking website of the same name that can be accessed at http://www.twitter.com. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users create and read 140-character messages called "Tweets," and to restrict their "Tweets" to individuals whom they approve. These features are described in more detail below.

101. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

102. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

103. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post "bios" of 160 characters or fewer to their profile pages.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

104. Twitter also keeps IP logs for each user. These logs contain information about the user's logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

105. As discussed above, Twitter users can use their Twitter accounts to post "Tweets" of 140 characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also "favorite," "retweet," or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the user with a list of other users who have "favorited" or "retweeted" the user's own Tweets, as well as a list of all Tweets that include the user's username (i.e., a list of all "mentions" and "replies" for that username).

106. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.

107. Twitter users can also opt to include location data in their Tweets, which will reveal the users' locations at the time they post each Tweet. This "Tweet With Location" function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.

108. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter's link service, which converts the longer website link into a shortened link that begins with http://t.co. This link service measures how many times a link has been clicked.

109. A Twitter user can "follow" other Twitter users, which means subscribing to those users' Tweets and site updates. Each user profile page includes a list of the people who are following that user (i.e., the user's "followers" list) and a list of people whom that user follows (i.e., the user's "following" list). Twitters users can "unfollow" users whom they previously followed, and they can also adjust the privacy settings for

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into "lists" that display on the right side of the user's home page on Twitter. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

110. In addition to posting Tweets, a Twitter user can also send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter's database.

111. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user's mobile phone, and the user can also set up a "sleep time" during which Twitter updates will not be sent to the user's phone.

112. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.

113. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles.

114. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.

115. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

116. As explained herein, information stored in connection with a Twitter account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Twitter user's account information, IP log, stored electronic communications, and other data retained by Twitter, can indicate who has used or controlled the Twitter account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, communications, "tweets" (status updates) and "tweeted" photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Twitter account at a relevant time. Further, Twitter account activity can show how and when the account was accessed or used. For example, as described herein, Twitter logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crime under investigation. Additionally, Twitter builds geo-location into some of its services. If enabled by the user, physical location is automatically added to "tweeted" communications. This geographic and timeline information may tend to either inculpate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner's state of mind as it relates to the offense under investigation. For example, information on the Twitter account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a criminal

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

117. Therefore, the computers of Twitter are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

XI. PAST EFFORTS TO OBTAIN THIS EVIDENCE

118. A search warrant was issued to Google, Inc. for information contained in and associated with the email account, robbcrson@gmail.com on December 19, 2016. This search warrant covered the time period January 1, 2013 to December 19, 2016. In their response, Google, Inc. did not include any email messages with attachments, stating they could not be certain the attachments were stored in the United States. Since that warrant was issued, Google, Inc. has informed the Government that, for future warrants, it will produce all information under its control that is responsive to the warrant, regardless of whether that information is stored in the United States or overseas. There had been no prior attempts to obtain information contained in or associated with the robbcrson@gmail.com account since December 19, 2016.

119. A search warrant was issued to Yahoo!, Inc. on December 19, 2016 for information contain in and associated with the email accounts mailpami4ever@yahoo.com and williamdotson38@yahoo.com. This search warrant covered the time period January 1, 2013 to December 19, 2016. Based on the information provided by Yahoo!, Inc., I know that the mailpami4ever@yahoo.com account was opened on February 19, 2007. Evidence of the user's identity is important in this case, and I believe any messages from outside the previously requested time period may contain this evidence.

120. Subpoenas have been issued to Facebook, Inc., Instagram, LLC, and Twitter, Inc. for subscriber information on some of the SUBJECT ACCOUNTS. However, information obtained by this method does not include records of stored

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

communications or other accounts that may be associated with the SUBJECT ACCOUNTS. For the reasons set out above, I believe that this additional information may contain evidence as to the identity of the users of the accounts, their co-conspirators, their location, and the actual conduct in which they engaged over the course of the criminal scheme.

121. On November 8, 2017, I submitted preservation letters to all of the SERVICE PROVIDERS requesting that they preserve information on the SUBJECT ACCOUNTS.

XII. REQUEST FOR SEALING

122. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

XIII. CONCLUSION

123. Based on the forgoing, I believe there is probable cause that evidence, fruits, and instrumentalities of the of violations of Title 18 U.S.C. §371 (conspiracy), §641 (theft of public money), §1028A (aggravated identity theft), and §1343 (wire fraud) are located in the SUBJECT ACCOUNTS, as more fully described in Attachment A-1 through A-5 to this Affidavit. I therefore request that the Court issue a warrant authorizing a search of the SUBJECT ACCOUNTS, for the items more fully described in Attachments B-1 through B-5 hereto, incorporated herein by reference, and the seizure of any such items found therein.

Eric Hergert, Affiant
Special Agent
I.R.S. Criminal Investigation

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on the 14th day of November, 2017.

Brian A. Tsuchida
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-1

Property to Be Searched

This warrant applies to information associated with the Gmail email addresses below, including all preserved data associated with the accounts and all subscriber and log records associated with the accounts, which are located at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered in Mountain View, California:

- robbcrson@gmail.com
- Robbcrson01@gmail.com
- smtpreceiverinbox@gmail.com
- Palmer.eloho.blogger@gmail.com
- officialnomzky@gmail.com
- nomzkysdmusiq@gmail.com

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-2

Property to Be Searched

This warrant applies to information associated with the Yahoo!, Inc. email addresses below, including all preserved data associated with the accounts and all subscriber and log records associated with the accounts, which are located at premises owned, maintained, controlled, or operated by Yahoo!, Inc., a company headquartered in Sunnyvale, California:

- mailpami4ever@yahoo.com
- Williamdotson38@yahoo.com
- nomzkysdm@yahoo.com
- onomen4us@yahoo.com

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-3
Property to Be Searched

This warrant applies to information associated with the Instagram accounts listed below that are stored at premises owned, maintained, controlled, or operated by Instagram, LLC, a company headquartered in San Francisco, California and owned by Facebook Inc., a company headquartered in Menlo Park, California.

- The Instagram accounts associated with the email address mailpami4ever@yahoo.com, including the account with the profile identification number 4268933941;
- The Instagram accounts associated with the email address nomzkymusiq@gmail.com, including the account with the profile identification number 209706106.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-4

Property to Be Searched

This warrant applies to information associated with the Facebook accounts listed below that are stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

- The Facebook accounts associated with the email address mailpami4ever@yahoo.com, including the account with the profile identification number 674058280;
- The Facebook accounts associated with the email address onomen4us@yahoo.com, including the account with the profile identification number 696285991.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-5
Property to Be Searched

This warrant applies to information associated with the Twitter accounts listed below that are stored at premises owned, maintained, controlled, or operated by Twitter, Inc., a company headquartered in San Francisco, California.

- The Twitter accounts associated with the email address mailpami4ever@yahoo.com, including the account with the user name (or "handle") "@palmerjoel88."
- The Twitter accounts associated with the email address, officialnomzky@gmail.com, including the account with the account ID: 138361510.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-1

Particular Things to Be Seized

I. Information to be disclosed by Google, Inc. (the Provider) for search:

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. §2703(f), the Provider is required to disclose the following information to the government, within fourteen (14) days of the issuance of this warrant:

a. The contents of all emails and instant messages associated with the account(s), including stored or preserved copies of emails or instant messages sent to and from the account(s) (including header information), draft emails or instant messages, deleted emails or instant messages which are still available, the source and destination addresses associated with each email or instant message, the date and time at which each email or instant message was sent, and the size and length of each email or instant message;

b. All records or other information regarding the identification of the account(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account(s) was created, the length of service, the IP address used to register the account(s), log-in IP addresses associated with session times

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and dates, account status, alternative email addresses provided, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service(s) utilized;

d. All records or other information stored at any time by an individual using the account(s), including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account(s), including contacts with support services and records of actions taken;

f. All records available regarding the location of the user of the account(s), including information obtained from IP addresses, GPS, wifi access points, or cell towers;

g. All records regarding device-specific information for devices used to access the accounts, including hardware model, operating system version, unique device identifiers, and mobile network information, including phone numbers;

h. Records of any other accounts associated with the SUBJECT ACCOUNTS through common cookies, device identifiers, email addresses, or phone numbers; and

i. Web and search history information for the accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

II. Information to be seized by the government:

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1028 (Identity Theft), 1028A (Aggravated Identity Theft), and 1343 (Wire Fraud), those violations occurring between January 1, 2013, and the present, including—for each account or identifier listed on Attachment A-1—information pertaining to the following matters:

1. All records, messages, documents, log files, and other information regarding the identity of the creator, user(s), or individual(s) controlling the identified accounts, and their past, present, or future location;
2. All records, messages, documents, log files, and other information regarding the identity of individuals being communicated with in regards to the above listed violations, and their past, present, or future location;
3. All messages, documents, and other information, including messages sent or received, all attachments, documents, or other information regarding:
    a. The impersonation of another individual, the transfer of information obtained from the impersonation of another individual, or the acquisition, transfer, or disposition of proceeds obtained from the impersonation of another individual;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Dating, match making, or similar websites, including communication with other individuals met through such websites, whether or not all communication ran through the websites;

c. The purchase, transfer, or sale of PII, including Forms W-2, lists of identity information, banking information, or tax information;

d. Instructions, usernames, passwords, and related information to be used in furthering identity theft and related fraudulent activities;

e. Forms W-2, tax returns, tax return preparation, bank accounts and prepaid debit cards, tax refunds, or information thereof;

f. The proceeds, expenses, or transfers of funds related to identity theft and related fraudulent activities;

g. Spam, phishing, hacking, concealing one's identity and online presence, and related cyber-crime activities;

4. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

5. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

6. Any address lists or buddy/contact lists associated with the specified accounts;

7. All subscriber records associated with the specified accounts, and any other accounts accessed from the same computers or digital devices, including:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. name,

b. address,

c. records of session times and durations,

d. length of service (including start date) and types of service utilized,

e. subscriber number or identity, including any temporarily assigned network address, and

f. means and source of payment for such service) including any credit card or bank account number; and

g. Any and all other historical log records, including IP address captures, associated with the specified accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-2

Particular Things to Be Seized

I. Information to be disclosed by Yahoo!, Inc. (the Provider):

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. §2703(f), the Provider is required to disclose the following information to the government, within fourteen (14) days of the issuance of this warrant:

a. The contents of all emails and instant messages associated with the account(s), including stored or preserved copies of emails or instant messages sent to and from the account(s) (including header information), draft emails or instant messages, deleted emails or instant messages which are still available, the source and destination addresses associated with each email or instant message, the date and time at which each email or instant message was sent, and the size and length of each email or instant message;

b. All records or other information regarding the identification of the account(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account(s) was created, the length of service, the IP address used to register the account(s), log-in IP addresses associated with session times

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and dates, account status, alternative email addresses provided, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service(s) utilized;

d. All records or other information stored at any time by an individual using the account(s), including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account(s), including contacts with support services and records of actions taken;

f. All records available regarding the location of the user of the account(s), including information obtained from IP addresses, GPS, wifi access points, or cell towers;

g. All records regarding device-specific information for devices used to access the accounts, including hardware model, operating system version, unique device identifiers, and mobile network information, including phone numbers;

h. Records of any other accounts associated with the SUBJECT ACCOUNTS through common cookies, device identifiers, email addresses, or phone numbers; and

i. Web and search history information for the accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

II. Information to be seized by the government:

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1028 (Identity Theft), 1028A (Aggravated Identity Theft), and 1343 (Wire Fraud), those violations occurring between January 1, 2013, and the present, including—for each account or identifier listed on Attachment A-2—information pertaining to the following matters:

1. All records, messages, documents, log files, and other information regarding the identity of the creator, user(s), or individual(s) controlling the identified accounts, and their past, present, or future location;
2. All records, messages, documents, log files, and other information regarding the identity of individuals being communicated with in regards to the above listed violations, and their past, present, or future location;
3. All messages, documents, and other information, including messages sent or received, all attachments, documents, or other information regarding:
    a. The impersonation of another individual, the transfer of information obtained from the impersonation of another individual, or the acquisition, transfer, or disposition of proceeds obtained from the impersonation of another individual;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Dating, match making, or similar websites, including communication with other individuals met through such websites, whether or not all communication ran through the websites;

c. The purchase, transfer, or sale of PII, including Forms W-2, lists of identity information, banking information, or tax information;

d. Instructions, usernames, passwords, and related information to be used in furthering identity theft and related fraudulent activities;

e. Forms W-2, tax returns, tax return preparation, bank accounts and prepaid debit cards, tax refunds, or information thereof;

f. The proceeds, expenses, or transfers of funds related to identity theft and related fraudulent activities;

g. Spam, phishing, hacking, concealing one's identity and online presence, and related cyber-crime activities;

4. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

5. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

6. Any address lists or buddy/contact lists associated with the specified accounts;

7. All subscriber records associated with the specified accounts, and any other accounts accessed from the same computers or digital devices, including:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. name,

b. address,

c. records of session times and durations,

d. length of service (including start date) and types of service utilized,

e. subscriber number or identity, including any temporarily assigned network address, and

f. means and source of payment for such service) including any credit card or bank account number; and

g. Any and all other historical log records, including IP address captures, associated with the specified accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-3

Particular Things to be Seized

I. Information to be disclosed by Instagram, LLC

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Instagram, LLC, including any messages, records, files, logs, or information that have been deleted but are still available to Instagram, LLC, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Instagram, LLC is required to disclose the following information to the government for each account identified in Attachment A-3, within fourteen (14) days of the issuance of this warrant:

(a) All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers;

(b) All past and current usernames associated with the account;

(c) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

(d) All activity logs including IP logs and other documents showing the IP address, date, and time of each login to the account, as well as any other log file information;

(e) All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie information, including all information about the particular device or devices used to access the account and the date and time of those accesses;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(f) All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

(g) All communications or other messages sent or received by the account;

(h) All user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other content;

(i) All photographs and images in the user gallery for the account;

(j) All location data associated with the account, including geotags;

(k) All data and information that has been deleted by the user;

(l) A list of all of the people that the user follows on Instagram and all people who are following the user (*i.e.*, the user's "following" list and "followers" list), as well as any friends of the user;

(m) A list of all users that the account has "unfollowed" or blocked;

(n) All privacy and account settings;

(o) All records of Instagram searches performed by the account, including all past searches saved by the account;

(p) All information about connections between the account and third-party websites and applications; and,

(q) All records pertaining to communications between Instagram, LLC and any person regarding the user or the user's Instagram account, including contacts with support services, and all records of actions taken, including suspensions of the account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §371 (conspiracy), §641 (theft of public money), §1028A (aggravated identity theft), and §1343 (wire fraud), including, for each account identified on Attachment A-3, information pertaining to the following matters:

(a) Communications regarding email spam, impersonation attempts, Form W-2 theft, United States tax returns, movement of tax refunds or other money within or from the United States, United States based bank accounts or prepaid debit card accounts, or other communication relevant to conducting the above violations, including evidence regarding the identity and location of the individuals involved in the communication;

(b) Evidence indicating how and when the Instagram account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Instagram account owner;

(c) Evidence indicating the Instagram account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID, including records that help reveal their whereabouts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-4
Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A-4 is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each account identified in Attachment A-4, within fourteen (14) days of the issuance of this warrant:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(i) All information about the Facebook pages that the account is or was a "fan" of;

(j) All past and present lists of friends created by the account;

(k) All records of Facebook searches performed by the account;

(l) All information about the user's access and use of Facebook Marketplace;

(m) The types of service utilized by the user;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §371 (conspiracy), §641 (theft of public money), §1028A (aggravated identity theft), and §1343 (wire fraud), including, for each account identified on Attachment A-4, information pertaining to the following matters:

(a) Communications regarding email spam, impersonation attempts, Form W-2 theft, United States tax returns, movement of tax refunds or other money within or from the United States, United States based bank accounts or prepaid debit card accounts, or other communication relevant to conducting the above violations, including evidence regarding the identity and location of the individuals involved in the communication;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(b) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;

(c) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the past, present, or future location of such person(s).

(e) The identity of the person(s) who communicated with the user ID, including records that help reveal their whereabouts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-5
Particular Things to Be Seized

I. Information to be disclosed by Twitter

To the extent that the information described in Attachment A-5 is within the possession, custody, or control of Twitter, including any messages, records, files, logs, or information that have been deleted but are still available to Twitter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each account listed in Attachment A-5, within fourteen (14) days of the issuance of this warrant:

(a) All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

(b) All past and current usernames, account passwords, and names associated with the account;

(c) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

(d) All IP logs and other documents showing the IP address, date, and time of each login to the account;

(e) All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(f) All "Tweets" and Direct Messages sent, received, "favorited," or retweeted by the account, and all photographs or images included in those Tweets and Direct Messages;

(g) All information from the "Connect" tab for the account, including all lists of Twitter users who have favorited or retweeted Tweets posted by the account, as well as a list of all Tweets that include the username associated with the account (*i.e.*, "mentions" or "replies");

(h) All photographs and images in the user gallery for the account;

(i) All location data associated with the account, including all information collected by the "Tweet With Location" service;

(j) All information about the account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;

(k) All data and information that has been deleted by the user;

(l) A list of all of the people that the user follows on Twitter and all people who are following the user (*i.e.*, the user's "following" list and "followers" list);

(m) A list of all users that the account has "unfollowed" or blocked;

(n) All "lists" created by the account;

(o) All information on the "Who to Follow" list for the account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(p) All privacy and account settings;

(q) All records of Twitter searches performed by the account, including all past searches saved by the account;

(r) All information about connections between the account and third-party websites and applications;

(s) All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §371 (conspiracy), §641 (theft of public money), §1028A (aggravated identity theft), and §1343 (wire fraud), including, for each account identified on Attachment A-5, information pertaining to the following matters:

a. Communications regarding email spam, impersonation attempts, Form W-2 theft, United States tax returns, movement of tax refunds or other money within or from the United States, United States based bank accounts or prepaid debit card accounts, or other communication relevant to conducting the above violations, including evidence regarding the identity and location of the individuals involved in the communication;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Evidence indicating how and when the Twitter account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Twitter account owner;

c. Evidence indicating the Twitter account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the user ID, including records that help reveal their whereabouts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

EXHIBIT A

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

GOOGLE, INC. EMAIL ACCOUNTS MORE FULLY DESCRIBED IN ATTACHMENT A-1

Case No. MJ16-531

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See attachment A1, attached hereto and incorporated herein by reference

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B1, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1028(a)(7)	Identity Theft;
18 U.S.C. § 1028A	Aggravated Identity Theft;
18 U.S.C. § 1343	Wire Fraud

The application is based on these facts:

See Affidavit of Eric Hergert, IRS-CI, attached hereto and incorporated herein by reference

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Eric Hergert

Applicant's signature

Eric Hergert, IRS-CI Special Agent

Printed name and title

Sworn to me pursuant to CrimRule 4.1.

Date: 12/19/16

Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, United States Magistrate Judge

Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Eric Hergert, a Special Agent with IRS Criminal Investigation in Tacoma, Washington, having been duly sworn, state as follows:

AFFIANT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the following email accounts (SUBJECT EMAIL ACCOUNTS):

a. Head.offices@execs.com
b. robbcrson@gmail.com
c. Mailpami4ever@yahoo.com
d. Williamdotson38@yahoo.com
e. smtpreceiverinbox@gmail.com

as well as all other email accounts linked to the SUBJECT EMAIL ACCOUNTS through the same phone number or alternate email address used during account registration (collectively, LINKED TARGET ACCOUNTS).

2. The information associated with the SUBJECT EMAIL ACCOUNTS and LINKED TARGET ACCOUNTS are stored at premises controlled by the following companies (collectively the EMAIL PROVIDERS):

a. Google, Inc., an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043;
b. 1&1 Mail & Media, Inc., an email provider headquartered at 701 Lee Road, Suite 300, Chesterbrook, PA 19087;
c. Yahoo!, Inc., an email provider headquartered at 701 First Avenue, Sunnyvale, CA 94089; or

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

3. The information to be searched is described in the following paragraphs and in Attachments A-1 through A-3 (collectively Attachments A). This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the EMAIL PROVIDERS to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachments B-1 through B-3 (collectively Attachments B). Upon receipt of the information described in Section I of Attachments B, government-authorized persons will review that information to locate the items described in Section II of Attachments B.

4. I am a Special Agent with Internal Revenue Service, Criminal Investigation (IRS-CI), and have been so employed since September 2009. I am presently assigned to IRS-CI's Seattle Field Office. My duties and responsibilities include the investigation of possible criminal violations of the Internal Revenue laws (Title 26, United States Code), the Bank Secrecy Act (Title 31, United States Code), the Money Laundering Control Act of 1986 (Title 18, United States Code, Sections 1956 and 1957), and other related offenses.

5. I earned a Bachelor of Arts degree in accounting from the University of Washington, Tacoma in 2002. I attended the Criminal Investigator Training Program and the Internal Revenue Service (IRS) Special Agent Basic Training at the Federal Law Enforcement Training Center where I received detailed training in conducting financial investigations. The training included search and seizure, violations of the Internal Revenue laws, and IRS procedures and policies in criminal investigations. Before being hired by IRS-CI, I was employed as a Revenue Agent for the IRS for approximately five years, performing civil examinations of small businesses and self-employed individuals. As a Revenue Agent, I received approximately 16 weeks of specialized training in personal, partnership, and corporate income tax, as specified in the Internal Revenue Code.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

6. I have conducted and assisted in several investigations involving financial crimes. I have led and participated in search warrants and have interviewed witnesses and defendants who were involved in, or had knowledge of, violations of the Internal Revenue Code, the Bank Secrecy Act, and the Money Laundering Control Act. In the course of my employment with IRS-CI, I have conducted or been involved in investigations of alleged criminal violations, which have included tax evasion (26 U.S.C. § 7201), filing a false tax return (26 U.S.C. § 7206(1)), aiding or assisting in the preparation of false tax returns (26 U.S.C. § 7206(2)), conspiring to defraud the United States (18 U.S.C. § 371), wire and mail fraud (18 U.S.C. § 1343 and § 1341), aggravated identity theft (18 U.S.C. § 1028A), and money laundering (18 U.S.C. § 1956 and § 1957), among others.

7. I have conducted and assisted in several investigations involving Stolen Identity Refund Fraud (SIRF) since 2010. I have been the Questionable Refund Program Coordinator for the IRS Criminal Investigation Seattle Field office since August 2013. As part of my duties in this position I have been responsible for receiving, researching, and reviewing leads involving false refund schemes, many of which involve the use of stolen identities, as well as assisting other agents in the field office with these types of cases. In my role as Questionable Refund Program Coordinator, I have attended specialized training put on by IRS Criminal Investigation each year since 2013. These training sessions have been multiple days, both in person and via webcast. Additionally, I attend monthly conference calls with others in my position during which we discuss current SIRF trends.

8. I have led and participated in the execution of Federal search warrants and the consensual searches of records relating to the concealment of assets and proceeds derived from fraud. These records included, but were not limited to, emails, instant messages, personal telephone books, photographs, bank records, escrow records, credit card records, tax returns, business books and records, and computer hardware and software.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

9. The information provided in this affidavit is supported by my training, experience, education, and participation in this and other financial and identity theft investigations.

10. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, review of documents and records related to this investigation, communication with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. The information provided in this affidavit is supported by my training, experience, education, and participation in this and other financial investigations.

11. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that violations of Title 18 U.S.C. §371 (Conspiracy), §1028(a)(7) (Identity Theft), §1028A (Aggravated Identity Theft), and §1343 (Wire Fraud) have been committed by unknown persons. There is also probable cause to search the information described in Attachments A for evidence of these crimes further described in Attachments B.

JURISDICTION

12. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§2703(a), (b)(1)(a), and (c)(1)(a). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offenses being investigated." 18 U.S.C. § 2711(3)(a)(i).

DEFINITION OF TERMS

13. The term "phishing" is defined by Merriam-Webster as "a scam by which an email user is duped into revealing personal or confidential information which the scammer can use illicitly."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

14. An "email header" is text at the beginning of an email message. It is generated by the client mail program that first sends it and updated by all the mail servers en route to the destination. Each mail server adds more text, including from/to addresses, subject, content type, time stamp and identification data. You can trace the path of the message from source to destination by reviewing the email header text. Many end user email programs hide this information from the user unless they specifically request to view it.

15. An internet cookie file, or "cookie," is a file that a website stores on a user's computer. The website can read the "cookie" and collect information about the computer on which the cookie has been saved. For example, a cookie might be used to track a user's account on the website, a user's preferences, or items in the user's electronic shopping cart.

THE INVESTIGATION

A. Summary

16. Beginning in approximately February 2016, IRS-CI began receiving reports from several companies across the nation regarding a phishing scheme in which unknown individuals impersonated CEOs, business owners, superintendents, or other high level management figures in emails sent to employees working in human resources or payroll processing. These emails requested the identity and payroll information of all company employees, often specifically requesting Form W-2 information. In many instances, the human resources or payroll processing employee believed the phishing emails actually came from senior management and replied to the email with the requested information, thereby sharing the identity and payroll information for company employees with the perpetrators of the phishing scheme. In many cases, the perpetrators of the fraud then used the personal information to file fraudulent tax returns and request tax refunds.

17. The users of the SUBJECT EMAIL ACCOUNTS and LINKED TARGET ACCOUNTS are not known at this time.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

B. Details of the Investigation

Kidder Mathews and Related Phishing Attacks

18. On March 22, 2016, P.O., the corporate controller for Kidder Mathews, LLC, contacted me to report a phishing attack against Kidder Mathews, LLC directed at the Human Resources manager, J.D. She provided copies of the email traffic between the J.D. and the individual(s) conducting the phishing attack. At all times during the email communication, J.D. was located in Western Washington.

19. Records provided by P.O. show that on March 21, 2016, J.D. received an email that appeared to be from J.L., the CEO of Kidder Mathews, LLC. The email asked J.D., "Could you please email me a Pdf copy of all employees' 2015 W-2s? I would like to make a quick review."

20. Other records provided by Kidder Mathews, LLC show that J.D. replied to the email the same day, noting that she was unable to access the Form W-2 information until the following day. A short time later, she received another email that appeared to be from J.L. indicating that a response the following day was fine, and to send a copy of the Form W-2 information to head.offices@execs.com (SUBJECT EMAIL ACCOUNT (a)).

21. The next day—on March 22, 2016—J.D. received an email that appeared to be from J.L. reminding her to complete the previous day's request and to send a copy to head.quarters@execs.com.

22. I reviewed the email header information for the emails sent to J.D. on March 21, 2016 and March 22, 2016 which appeared to be from J.L. I was able to determine that these emails were not sent from J.L.'s company email account, and that J.D. was actually corresponding with an individual(s) using the email account head.quarters@execs.com.

23. March 22, 2016, J.D. sent two emails containing Forms W-2 for employees of Kidder Mathews, LLC and Kidder Mathews of California. These emails were sent to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

J.L. at his correct company email address, with a copy sent to an unknown individual(s) at the email address, head.quarters@execs.com.

24. According to information obtained from Kidder Mathews, LLC, the personally identifiable information (PII) and 2015 payroll information for approximately 352 employees of Kidder Mathews, LLC and Kidder Mathews of California were included in J.D.'s replies to the phishing attacks.

25. After the phishing attacks, the IRS identified several fraudulent and suspicious tax returns filed using the identities of Kidder Mathews, LLC and Kidder Mathews of California employees. Between March 22, 2016, and October 15, 2016, the IRS received approximately 150 tax returns for individuals reporting wages from Kidder Mathews, LLC and Kidder Mathews of California. As of November 9, 2016, the IRS determined that at least 51 of the returns are fraudulent and another 24 are suspicious and pending further review due to potential identity theft concerns. These 75 fraudulent and suspicious tax returns were all filed electronically and claimed refunds totaling $300,313.

26. On May 5, 2016, I served a search warrant on 1&1 Mail & Media, Inc. for information contained within the email account head.quarters@execs.com. Information obtained from this search warrant showed the email account was created on March 21, 2016, and helped to identify other companies who were tricked into providing their employees' identity and payroll information, including Idexcel, Inc. and Alpine Learning Group, Inc.

27. A search of the records obtained from the search warrant on head.quarters@execs.com found that on March 21, 2016, an email was sent to S.N. at Idexcel, Inc. asking, "Could you please email me a Pdf copy of all employees' 2015 W-2s? I would like to make a quick review." This is the same language that was used in the email sent to J.D. at Kidder Mathews, LLC. The email to S.N. appeared to be from P.A., the CEO of Idexcel, Inc., through an Idexcel, Inc. email address. However, when S.N. replied to the email with Form W-2 information for approximately 534 employees on

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

March 21, 2016, the information was actually sent to the email account, head.quarters@execs.com.

28. Between March 21, 2016 and October 18, 2016, the IRS received approximately 216 tax returns that included a Form W-2 reporting income from Idexcel, Inc. As of November 9, 2016, the IRS determined that 44 of the tax returns are fraudulent and an additional 25 are suspicious and pending further review due to potential identity theft concerns. These 69 fraudulent and suspicious tax returns were all filed electronically and claimed refunds totaling $305,575.

29. On March 21, 2016, an email was sent to L.M. at Alpine Learning Group, Inc. asking, "Could you please email me a Pdf copy of all employees' 2015 W-2s? I would like to make a quick review." This is the same language that was used in the email sent to J.D. at Kidder Mathews, LLC and S.N. at Idexcel, Inc. The email to L.M. appeared to be from M.B., the president of Alpine Learning Group, Inc., through an Alpine Learning Group, Inc. email address. However, when L.M. replied to the email she was actually communicating with someone using the email account, head.quarters@execs.com.

30. L.M originally replied to the email stating she was "uncomfortable emailing this confidential information containing employees' Social Security numbers and birthdates, as our email is not encrypted and the information would not be secure."

31. The same day, L.M. received a reply to her email which also appeared to be from M.B. that stated, "Thank you for your 2cents but this request begins right where your comfort ends due to the fact that an external audit process is being carried out by the board which requires the requested employees' information in sight. Let the board worry about encryption and whatnot . Kindly email me the requested documents omitting no detail." Another email was sent to L.M. a short time later requesting she send a copy of the information to head.offices@execs.com.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

32. L.M. replied to the email request with Form W-2 information for approximately 116 employees on March 21, 2016. However, the information was not sent to M.B., but was actually sent to the email account, head.quarters@execs.com.

33. Between March 21, 2016 and October 17, 2016, the IRS received approximately 58 tax returns that included a Form W-2 reporting income from Alpine Learning Group, Inc. As of November 9, 2016, the IRS determined that four of the tax returns are fraudulent and an additional 10 are suspicious and pending further review due to potential identity theft concerns. These 14 fraudulent and suspicious tax returns were all filed electronically and claimed refunds totaling $40,878.

34. According to information obtained in the search warrant, the Form W-2 information described above was sent from head.quarters@execs.com to other email accounts.

35. On March 21, 2016, head.quarters@execs.com sent the Form W-2 information for Idexcel, Inc. to robbcrson@gmail.com (SUBJECT EMAIL ACCOUNT (b)).

36. Head.quarters@execs.com sent the Form W-2 information for Idexcel, Inc., Alpine Learning Group, Inc., Kidder Mathews, LLC, and Kidder Mathews of California to mailpami4ever@yahoo.com (SUBJECT EMAIL ACCOUNT (c)) from March 21, 2016 to March 22, 2016.

Workforce Software and Related Phishing Attacks

37. On or about April 8, 2016, I talked with M.Mu., the Director of Security and Privacy at Workforce Software, LLC. He confirmed that Workforce Software, LLC was the victim of a phishing attack.

38. Records provided by M.Mu. show that, on March 7, 2016, L.T., the vice president of Human Resources at Workforce Software, LLC, received an email that appeared to be from M.Mo., the company's CEO. The email asked L.T., "Could you please forward me a pdf copy of all employees' W2s? I would like to make a quick

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

review." This is nearly the exact same language as that used in the email sent to J.D. at Kidder Mathews, LLC, S.N. at Idexcel, Inc., and L.M. at Alpine Learning Group, Inc.

39. I reviewed the email header information of the email sent to L.T. From that information, I was able to determine the email was not from M.Mo. Replies to the email were to be sent to the email account, headquarter@accountant.com.

40. On March 7, 2016, L.T. emailed Form W-2 information for approximately 455 Workforce Software, LLC employees to M.Mo. at his company email address and sent a copy to headquarter@accountant.com.

41. Between March 7, 2016, and October 17, 2016, the IRS received approximately 270 tax returns that included a Form W-2 reporting income from Workforce Software, LLC. As of July 19, 2016, the IRS determined that 101 of the tax returns are fraudulent and an additional 39 are suspicious and pending further review due to potential identity theft concerns. These 140 fraudulent and suspicious tax returns were all filed electronically and claimed refunds totaling $611,466.

42. I reviewed several tax returns filed with the IRS which reported wage income from Workforce Software, LLC. Five of the tax returns were for the individuals A.B., K.A., D.Al., N.A., and D.An. All five of these tax returns requested the refund be issued directly, or indirectly, to Wells Fargo account *5807. I spoke with K.A., D.Al., and D.An, and they confirmed the tax returns filed in their names were false and they did not authorize payment of their tax refunds to Wells Fargo account *5807.

43. On May 5, 2016, I served a search warrant on 1&1 Mail & Media, Inc. for information contained within the email account headquarter@accountant.com. Information obtained from this search warrant showed the email account headquarter@accountant.com was created on March 7, 2016 and helped to identify other companies that had been tricked into providing their employees' identity and payroll information, including MTE Corporation and ASF Logistics, Inc.

44. On March 7, 2016, an email was sent to K.W., a Human Resources assistant at MTE Corporation, asking, "Could you please forward me a pdf copy of all

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

employees' W2s? I would like to make a quick review." This is the same language that was used in the email sent to L.T. at Workforce Software, LLC. The email to K.W. appeared to be from D.K., the president of MTE Corporation through a company email address. However, when K.W. replied to the email with Form W-2 information for approximately 108 employees, the information was actually sent to the email account, headquarter@accountant.com.

45. Between March 7, 2016, and April 16, 2016, the IRS received approximately 43 tax returns that included a Form W-2 reporting income from MTE Corporation. As of November 9, 2016, the IRS determined that 13 of the tax returns are fraudulent and an additional two are suspicious and pending further review due to potential identity theft concerns. These 15 fraudulent and suspicious tax returns were all filed electronically and claimed refunds totaling $76,271.

46. On March 7, 2016, an email was sent to J.P. at ASF Logistics, Inc. asking, "Could you please forward me a pdf copy of all employees' W2s? I would like to make a quick review." This is the same language that was used in the email sent to L.T. at Workforce Software, LLC and K.W. at MTE Corporation. The email to J.P. appeared to be from S.C., the president of ASF Logistics, Inc. through a company email address. However, when K.W. replied to the email with Form W-2 information for approximately 33 employees, the information was actually sent to the email account, headquarter@accountant.com.

47. Between March 7, 2016, and April 18, 2016, the IRS received approximately 11 tax returns that included a Form W-2 reporting income from ASF Logistics, Inc. As of November 9, 2016, the IRS determined that six of the tax returns are fraudulent, and an additional two are suspicious and pending further review due to potential identity theft concerns. These eight fraudulent and suspicious tax returns were all filed electronically and claimed refunds totaling $37,479.

48. According to information obtained in the search warrant, the Form W-2 information described above was sent from headquarter@accountant.com to other email

accounts on March 7, 2016. Headquarter@accountant.com sent the Form W-2 information for MTE Corporation and ASF Logistics, Inc. to robbcrson@gmail.com (SUBJECT EMAIL ACCOUNT (b)), mailpami4ever@yahoo.com (SUBJECT EMAIL ACCOUNT (c)), and williamdotson38@yahoo.com (SUBJECT EMAIL ACCOUNT (d)). Headquarter@accountant.com sent the Form W-2 information for Workforce Software, LLC and MTE Corporation to smtpreceiverinbox@gmail.com (SUBJECT EMAIL ACCOUNT (e)).

49. In total, the IRS received approximately 321 fraudulent and suspicious tax returns filed for employees of the six companies that had Forms W-2 stolen in the above mentioned phishing schemes. These fraudulent and suspicious tax returns claimed refunds of approximately $1,371,982.

Additional Probable Cause for Email Accounts

50. Based on my training and experience, I know that stolen identity refund fraud is often conducted by groups of individuals. These individuals may be in different locations across the country or in different countries across the world. In order to conduct the scheme the coconspirators have to communicate. This communication is often done through text messages, emails, and instant messenger accounts.

51. From my background, I know that criminal organizations often use email, instant messaging, text messaging, and other forms of electronic communication to facilitate SIRF crimes. I have reviewed information obtained from search warrants of email and instant message accounts and know that these forms of communication are often used by identity thieves to obtain and transfer:

a. Identity theft victim PII, such as names, Social Security Numbers, addresses, and dates of birth;

b. Credit reports, income information, and prior year tax return information of identity theft victims;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. Passwords, PIN numbers, and other information required to file fraudulent tax returns in the names of identity theft victims;

d. Bank and prepaid debit card account numbers and passwords;

e. Instructions on how to obtain PII, file fraudulent returns, and access the fraudulent refunds; and

f. Instructions on how to disperse the fraudulent refunds received.

52. There are many reasons why criminal offenders maintain electronic communication evidence for long periods of time. Items such as identity theft victim PII have value, as they may be sold, used for other purposes, or reused for the same purpose in future years. Additionally, electronic communication is often stored on third party servers, and may not actually be deleted immediately, even if put into a "deleted items folder" or "trash." The criminal offender may no longer realize that they still possess the evidence or they may believe that law enforcement could not obtain a search warrant to seize the evidence.

53. In many instances, identity thieves also communicate with individuals not involved in the conspiracy for purposes of using them unwittingly in their scheme. For example, identity thieves will befriend individuals met through online dating sites and convince them to receive money from a source unknown to that person and forward it on to the identity thief. Although the identity thief usually uses a false identity in these email communications, the items being discussed could provide information or evidence that can be used to further identify the identity thief or trace the fraudulent refunds.

54. Based on my training and experience, I also know that identity thieves often use email to communicate about other matters that may provide evidence as to the identity and location of the individual(s) using the email accounts. I know that communications between identity thieves may also include identifying information about the users of the email or instant message accounts. For example, messages may include names, nicknames, locations, travel plans, or birthdays that can be used to identify the criminal offenders.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

55. Based on my training and experience, I know that individuals conducting phishing schemes, identity theft, and SIRF crimes often have several email addresses. The multiple email accounts are used because accounts often get closed by the email providers when they receive information regarding the email account being used in phishing schemes.

56. Email accounts used by the individuals conducting the phishing, identity theft, and tax fraud schemes for non-criminal communication may still contain evidence of the identity of the individual(s) using the SUBJECT EMAIL ACCOUNTS.

PAST EFFORTS TO OBTAIN THIS EVIDENCE

57. The evidence described in Attachments B has not been previously available to me or other agents.

58. Preservation letters were provided to the EMAIL PROVIDERS for these accounts on December 12, 2016.

BACKGROUND REGARDING EMAIL PROVIDER'S SERVICES

59. In my training and experience, I have learned that the EMAIL PROVIDERS provide the public with a variety of on-line services, including electronic mail ("email") access, to the public. The EMAIL PROVIDERS allow subscribers to obtain email accounts under various domain names, including gmail.com for Google, Inc., execs.com for 1&1 Mail and Media, Inc., and yaoo.com for Yahoo!, Inc., like the email accounts listed in Attachments A. Subscribers obtain an account by registering with the EMAIL PROVIDERS. During the registration process, the EMAIL PROVIDERS ask subscribers to provide basic personal information, which may include name, address, phone numbers, payment information, and other personal information. Therefore, the computers of the EMAIL PROVIDERS are likely to contain stored electronic communications (including retrieved and unretrieved email for the EMAIL PROVIDERS' subscribers) and information concerning subscribers and their use of the EMAIL PROVIDERS' services, such as account access information, email transaction information, and account application information. In my training and experience, such

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

60. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

61. In general, an email that is sent to an EMAIL PROVIDERS subscriber is stored in the subscriber's "mail box" on the EMAIL PROVIDERS' servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the EMAIL PROVIDERS' servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the EMAIL PROVIDERS' servers for a certain period of time.

62. When subscribers send emails, they are initiated at the users' computers, transferred via the Internet to the EMAIL PROVIDERS' servers, and then transmitted to their end destinations. The EMAIL PROVIDERS often maintain a copy of the email sent. Unless the email senders specifically delete the emails from the EMAIL PROVIDERS' servers, the emails can remain on the systems indefinitely. Even if the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

senders delete the emails, they may continue to be available on the EMAIL PROVIDERS' servers for a certain period of time.

63. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by the EMAIL PROVIDERS but may not include all of these categories of data.

64. Subscribers to the EMAIL PROVIDERS services can also store files, including emails, address books, contact or buddy lists, calendar data, photographs, and other files, on servers maintained and/or owned by the EMAIL PROVIDERS. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, attachments to emails, including photographs and files, and photographs and files stored in relation to the account.

65. A Yahoo, Inc. subscriber can also store files, including emails, address books, contact or buddy lists, calendar data, photographs, and other files, on servers maintained and/or owned by Yahoo, Inc. I know based on my training and experience and my review of Yahoo's services, that Yahoo! provides users with access to an address book in which they may store contact information including names, addresses, email address, and telephone numbers. Yahoo! also provides users access to a "Calendar" file that may include notes of events and schedules. Yahoo also provides users with access to a service called "Flicker" that can be used to create photo albums, store photographs, and share photographs with others. Yahoo! also provides users with access to Yahoo! Groups which allows users to share photographs, calendars and messages with others who typically share a common interest. In my training and experience, evidence of who was using an email account may be found in address books, calendars, photographs and other documents stored in relation to the account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

66. A subscriber to a Google Gmail account can also store files, including address books, contact lists, calendar data, photographs and other files, on servers maintained and/or owned by Google. For example, Google offers users a calendar service that users may utilize to organize their schedule and share events with others. Google also offers users' a service called Google Drive that may be used to store data and documents. The Google Drive service may be used to store documents including spreadsheets, written documents (such as Word or Word Perfect) and other documents that could be used to manage a website. Google Drive allows users to share their documents with others or the public depending on the settings selected by the account holder. Google also provides its users with access to the photo storage service "Picasa." Picasa can be used to create photo albums, store photographs, and share photographs with others. Another Google service called "You Tube" allows users to view, store and share videos. Google also provides a service called "Google Analytics. Google Analytics is a Google service that monitors website traffic and provides subscribers with data relating to how much traffic is visiting the subscriber's website, which sections of the subscriber's website users are visiting, how long users are staying on particular sections of the site, and the geographical source of users visiting the website, among other things.

67. Additionally, based on my training and experience, as well as Google, Inc.'s Privacy Policy, I know that Google, Inc. also collects information about users, including information about the devices on which they access their accounts, the devices' hardware models, operating system versions, unique device identifiers, and mobile network information including phone number, location information, and search queries. This information is evidence that can be used to identify and find the individuals conducting the fraud.

68. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

69. This application seeks a warrant to search all responsive records and information under the control of the EMAIL PROVIDERS, providers subject to the jurisdiction of this court, regardless of where the EMAIL PROVIDERs have chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within the EMAIL PROVIDERS' possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. [1]

70. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the

---

[1] It is possible that the EMAIL PROVIDERS store some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information— including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of the EMAIL PROVIDERS. The government also seeks the disclosure of the physical location or locations where the information is stored.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

71. Based on my training and experience, I know that some email providers, including the EMAIL PROVIDERS, often use internet cookie files to track user information. These "cookies" may allow the email providers to collect information about the account users' computers, including information about other accounts accessed by a computer containing the email provider's "cookie." Specifically, the EMAIL PROVIDERS may collect information about other email accounts with their service that were accessed by the computers that also accessed the email accounts described in Attachments A.

72. Information regarding other email accounts accessed from the same computer(s) that accessed the email accounts described in Attachments A may provide important evidence about the person using both accounts, including his/her identity and location, as well as the full extent of the fraud.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

73. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to permit the EMAIL PROVIDERS and their agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to the EMAIL PROVIDERS with direction that they identify the relevant account(s) described in Attachments A to this affidavit, as well as other subscriber and log records associated with the account, as set forth in Section I of Attachments B to this affidavit.

74. The search warrant will direct the EMAIL PROVIDERS to create an exact copy of the specified account and records.

75. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data, and identify from among that content those items that come within the items identified in Section II to Attachments B, for seizure.

76. Analyzing the data contained in the forensic image may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common email, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

methodologies reasonably designed to identify and seize the items identified in Section II of Attachments B to the warrant.

77. Based on my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize a variety of email communications, chat logs and documents, that identify any users of the subject account and emails sent or received in temporal proximity to incriminating emails that provide context to the incriminating communications.

REQUEST FOR NON-DISCLOSURE AND SEALING

78. The government requests, pursuant to the preclusion of notice provisions of Title 18, United States Code, Section 2705(b), that the EMAIL PROVIDERS be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for such period as the Court deems appropriate. The government submits that such an order is justified because notification of the existence of this Order would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution.

79. It is further respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation, and law enforcement may still attempt to execute additional search warrants before the investigation concludes. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

CONCLUSION

80. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a),

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(b)(1)(A) & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the warrant will be served on the EMAIL PROVIDERS, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. Accordingly, by this Affidavit and Warrant, I seek authority for the government to search all of the items specified in Section I, Attachments B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

Special Agent Eric Hergert, Affiant
IRS Criminal Investigation

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on the 19th day of December, 2016.

HONORABLE BRIAN A. TSUCHIDA
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Attachment A-1

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with Google, Inc. account:

a. robbcrson@gmail.com

b. smtpreceiverinbox@gmail.com

as well as all other email accounts linked to the identified accounts through the same phone number or alternate email address used during account registration, as well as all other subscriber and log records associated with the account, which are located at premises owned, maintained, controlled or operated by Google, Inc., an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Attachment A-2

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with 1&1 Mail & Media, Inc. accounts:

a. head.offices@execs.com

as well as all other email accounts linked to the identified accounts through the same phone number or alternate email address used during account registration, as well as all other subscriber and log records associated with the accounts, which are located at premises owned, maintained, controlled or operated by 1&1 Mail & Media, Inc., an email provider headquartered at 701 Lee Road, Suite 300, Chesterbrook, PA 19087.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Attachment A-3

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with Yahoo!, Inc. accounts:

a. mailpami4ever@yahoo.com

b. Williamdotson38@yahoo.com

as well as all other email accounts linked to the identified accounts through the same phone number or alternate email address used during account registration, as well as all other subscriber and log records associated with the accounts, which are located at premises owned, maintained, controlled or operated by Yahoo!, Inc., an email provider headquartered at 701 First Avenue, Sunnyvale, CA 94089.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Attachment B-1

Section I - Information to be disclosed by Google, Inc. (the Provider) for search:

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. §2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

a. The contents of all emails associated with the account(s), including stored or preserved copies of emails sent to and from the account(s) (including email header information), draft emails, deleted emails which are still available, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account(s) was created, the length of service, the IP address used to register the account(s), log-in IP addresses associated with session times and dates, account status, alternative email addresses provided, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service(s) utilized;

d. All records or other information stored at any time by an individual using the account(s), including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account(s), including contacts with support services and records of actions taken;

f. **For all other email accounts accessed from the same computer or device as the account(s) described in Attachment A-1**, subscriber information, including subscriber name, address, service types, IP address history, billing records, recovery email accounts and phone numbers, and dates and times of sessions;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. All records available regarding the location of the user of the account(s) described in attachment A-1, including information obtained from IP addresses, GPS, wifi access points, or cell towers;

h. All records regarding device-specific information for devices used to access the account described in Attachment A-1, including hardware model, operating system version, unique device identifiers, and mobile network information, including phone numbers; and

i. Web and search history information for the account in Attachment A-1.

j. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of the issuance of this warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Section II - Information to be seized by the government:

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1028 (Identity Theft), 1028A (Aggravated Identity Theft), and 1343 (Wire Fraud), those violations occurring between January 1, 2013, and the present, including—for each account or identifier listed on Attachment A-1—information pertaining to the following matters:

a. All messages, documents, and other information, including messages sent or received, all attachments, documents, or other information regarding:

1. The impersonation of another individual, the transfer of information obtained from the impersonation of another individual, or the acquisition, transfer, or disposition of proceeds obtained from the impersonation of another individual;

2. Dating, match making, or similar websites, including communication with other individuals met through such websites, whether or not all communication ran through the websites;

3. The purchase, transfer, or sale of PII, including Forms W-2, lists of identity information, banking information, tax information;

4. Instructions, usernames, passwords, and related information to be used in furthering identity theft and related fraudulent activities;

5. Forms W-2, tax returns, tax return preparation, bank accounts and prepaid debit cards, and tax refunds;

6. The proceeds, expenses, or transfers of funds related to identity theft and related fraudulent activities;

7. Spam, phishing, hacking, concealing one's identity and online presence, and related cyber-crime activities;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

8. Any other messages, documents, or other information that assists with identifying the individuals using or exercising dominion or control over the email accounts (sender and receiver) containing messages, documents, or information described above and their location;

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the user ID about matters relating to impersonation, identity theft, tax fraud, wire fraud, and money laundering, including records that help reveal their whereabouts.

f. Any address lists or buddy/contact lists associated with the specified accounts;

g. All subscriber records associated with the specified accounts, and any other accounts accessed from the same computers or digital devices, including:
   1. name,
   2. address,
   3. records of session times and durations,
   4. length of service (including start date) and types of service utilized,
   5. subscriber number or identity, including any temporarily assigned network address, and
   6. means and source of payment for such service) including any credit card or bank account number;

h. Any and all other historical log records, including IP address captures, associated with the specified accounts; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Attachment B-2

Section I - Information to be disclosed by 1&1 Mail & Media, Inc. (the Provider) for search:

a. The contents of all emails associated with the account(s), including stored or preserved copies of emails sent to and from the account(s) (including email header information), draft emails, deleted emails which are still available, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account(s) was created, the length of service, the IP address used to register the account(s), log-in IP addresses associated with session times and dates, account status, alternative email addresses provided, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service(s) utilized;

d. All records or other information stored at any time by an individual using the account(s), including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account(s), including contacts with support services and records of actions taken;

f. **For all other email accounts accessed from the same computer or device as the account(s) described in Attachment A-2**, subscriber information, including subscriber name, address, service types, IP address history, billing records, recovery email accounts and phone numbers, and dates and times of sessions;

g. All records available regarding the location of the user of the account(s) described in attachment A-2, including information obtained from IP addresses, GPS, wifi access points, or cell towers;

h. All records regarding device-specific information for devices used to access the account described in Attachment A-2, including hardware model, operating system version, unique device identifiers, and mobile network information, including phone numbers; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

i. Web and search history information for the account in Attachment A-2.

j. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of the issuance of this warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Section II - Information to be seized by the government:

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy) 1028 (Identity Theft), 1028A (Aggravated Identity Theft) and 1343 (Wire Fraud), those violations occurring between January 1, 2013, and the present, including—for each account or identifier listed on Attachment A-2—information pertaining to the following matters:

a. All messages, documents, and other information, including messages sent or received, all attachments, documents, or other information regarding:
   1. The impersonation of another individual, the transfer of information obtained from the impersonation of another individual, or the acquisition, transfer, or disposition of proceeds obtained from the impersonation of another individual;
   2. Dating, match making, or similar websites, including communication with other individuals met through such websites, whether or not all communication ran through the websites;
   3. The purchase, transfer, or sale of PII, including Forms W-2, lists of identity information, banking information, tax information;
   4. Instructions, usernames, passwords, and related information to be used in furthering identity theft and related fraudulent activities;
   5. Forms W-2, tax returns, tax return preparation, bank accounts and prepaid debit cards, and tax refunds;
   6. The proceeds, expenses, or transfers of funds related to identity theft and related fraudulent activities;
   7. Spam, phishing, hacking, concealing one's identity and online presence, and related cyber-crime activities;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

8. Any other messages, documents, or other information that assists with identifying the individuals using or exercising dominion or control over the email accounts (sender and receiver) containing messages, documents, or information described above and their location;

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the user ID about matters relating to impersonation, identity theft, tax fraud, wire fraud, and money laundering, including records that help reveal their whereabouts.

f. Any address lists or buddy/contact lists associated with the specified accounts;

g. All subscriber records associated with the specified accounts, and any other accounts accessed from the same computers or digital devices, including:
   1. name,
   2. address,
   3. records of session times and durations,
   4. length of service (including start date) and types of service utilized,
   5. subscriber number or identity, including any temporarily assigned network address, and
   6. means and source of payment for such service) including any credit card or bank account number; and

h. Any and all other historical log records, including IP address captures, associated with the specified accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Attachment B-3

Section I - Information to be disclosed by Yahoo!, Inc. (the Provider) for search:

a. The contents of all emails associated with the account(s), including stored or preserved copies of emails sent to and from the account(s) (including email header information), draft emails, deleted emails which are still available, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account(s) was created, the length of service, the IP address used to register the account(s), log-in IP addresses associated with session times and dates, account status, alternative email addresses provided, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service(s) utilized;

d. All records or other information stored at any time by an individual using the account(s), including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account(s), including contacts with support services and records of actions taken;

f. **For all other email accounts accessed from the same computer or device as the account(s) described in Attachment A-3**, subscriber information, including subscriber name, address, service types, IP address history, billing records, recovery email accounts and phone numbers, and dates and times of sessions;

g. All records available regarding the location of the user of the account(s) described in attachment A-3, including information obtained from IP addresses, GPS, wifi access points, or cell towers;

h. All records regarding device-specific information for devices used to access the account described in Attachment A-3, including hardware model, operating system version, unique device identifiers, and mobile network information, including phone numbers; and

i. Web and search history information for the account in Attachment A-3.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

j. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of the issuance of this warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Section II - Information to be seized by the government:

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 371 (Conspiracy), 1028 (Identity Theft), 1028A (Aggravated Identity Theft) and 1343 (Wire Fraud), those violations occurring between January 1, 2013, and the present, including—for each account or identifier listed on Attachment A-3—information pertaining to the following matters:

a. All messages, documents, and other information, including messages sent or received, all attachments, documents, or other information regarding:

1. The impersonation of another individual, the transfer of information obtained from the impersonation of another individual, or the acquisition, transfer, or disposition of proceeds obtained from the impersonation of another individual;

2. Dating, match making, or similar websites, including communication with other individuals met through such websites, whether or not all communication ran through the websites;

3. The purchase, transfer, or sale of PII, including Forms W-2, lists of identity information, banking information, tax information;

4. Instructions, usernames, passwords, and related information to be used in furthering identity theft and related fraudulent activities;

5. Forms W-2, tax returns, tax return preparation, bank accounts and prepaid debit cards, and tax refunds;

6. The proceeds, expenses, or transfers of funds related to identity theft and related fraudulent activities;

7. Spam, phishing, hacking, concealing one's identity and online presence, and related cyber-crime activities;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

8. Any other messages, documents, or other information that assists with identifying the individuals using or exercising dominion or control over the email accounts (sender and receiver) containing messages, documents, or information described above and their location;

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the user ID about matters relating to impersonation, identity theft, tax fraud, wire fraud, and money laundering, including records that help reveal their whereabouts.

f. Any address lists or buddy/contact lists associated with the specified accounts;

g. All subscriber records associated with the specified accounts, and any other accounts accessed from the same computers or digital devices, including:
   1. name,
   2. address,
   3. records of session times and durations,
   4. length of service (including start date) and types of service utilized,
   5. subscriber number or identity, including any temporarily assigned network address, and
   6. means and source of payment for such service) including any credit card or bank account number;

h. Any and all other historical log records, including IP address captures, associated with the specified accounts; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970